REMARKS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-4 and 7-12 are pending in the present application. Claims 1, 4, 7, 8, and 10-12 are amended without the introduction of any new matter, and Claims 5 and 6 are canceled without prejudice or disclaimer by the present amendment.

In the outstanding Office Action, Claims 1, 2, and 10 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,240,432 to Chuang et al. (hereinafter "Chuang"); Claim 3 was rejected under 35 U.S.C. § 103(a) as unpatentable over Chang in view of U.S. Patent No. 6,522,210 to Dvorak et al. (hereinafter "Dvorak"); Claims 11 and 12 were rejected under § 103(a) as unpatentable over Chuang in view of U.S. Patent No. 6,480,072 to Walsh et al. (hereinafter "Walsh"); Claims 1-3, 5-7, and 10-12 were rejected under § 103(a) as unpatentable over Walsh in view of U.S. Patent No. 4,799,259 to Ogrodski; and Claims 4, 8, and 9 were indicated as allowable if rewritten in independent form.

Applicant thanks the examiner for the indication of allowable subject matter. In view thereof, Claims 4 and 8 are rewritten in independent form to include all of the limitations of the base claim and any intervening claims. Claim 9 depends from Claim 8.

Claims 1-3 and 10-12 stand rejected under § 102(e) and § 103(a) as anticipated by or unpatentable over Chuang. As independent Claims 1, 11, and 12 are amended to incorporate the subject matter of dependent Claims 5 and 6, those rejections are moot. Accordingly, Applicant respectfully requests that those rejections be withdrawn.

Claims 1-3, 5-7, and 10-12 stand rejected as unpatentable over Walsh in view of Ogrodski. That rejection is respectfully traversed.

Amended Claim 1 is directed to a digital true random number generator circuit. The circuit includes:

> a linear feedback shift register having an input and an output;
>
> a plurality of free-running oscillators each operatively connected to a separate input of a single exclusive OR-circuit;
>
> said exclusive OR-circuit having an output operatively connected to an input of a latching circuit;
>
> said latching circuit having an output operatively connected to the input of said linear feedback shift register and configured to drive said linear feedback shift register; and
>
> a system clock operatively connected to a clock input of said latching circuit and having a system clock frequency value configured to drive said linear feedback shift register,
>
> wherein said free-running oscillators and said system clock have different oscillation frequency values, the greatest common divisor of the different oscillation frequency values having the value one.

Amended independent Claims 10-12 recite a similar digital true random number generator circuit. Claims 2, 3, and 7 depend from Claim 1.

By way of background, a linear feedback shift register ("LFSR") may be driven by a frequency signal delivered from a free-running oscillator.[1] More particularly, the frequency signal provides a noise signal that disrupts the generation of pseudo-random numbers by the LFSR, thereby making the generated random numbers more truly random.[2] However, due to temperature and other factors, oscillation devices may "lock" onto system clocks.[3] When such locking occurs, the random numbers generated by the LFSR become more predictable.[4] The claimed invention is provided, in part, in view of this deficiency.

In a non-limiting example, Figure 1 illustrates an embodiment of the claimed invention. As shown, the ring oscillators 10, 20, 30 each separately input to a single XOR-circuit 1; the output signal 1a of the single XOR-circuit 1 inputs to a latching circuit 2, which is triggered by a single clock pulse 3a; and the output of the latching circuit 2 serves as the

[1] Specification, page 1, line 31 – page 2, line 2.
[2] Specification, page 2, lines 2-4.
[3] Specification, page 2, lines 5-9.
[4] Specification, page 2, lines 9-11.

input for the LFSR circuit 4. By this configuration, the frequency of the output signal of the XOR-circuit 1 is unaffected by the system clock pulse fed to the latching circuit 2. Consequently, as the locking of the several oscillating devices 10, 20, 30 on one single clock pulse is prevented, the generation of pseudo-random numbers is reduced.[5]

The outstanding Office Action cites the CRC circuit 117, sample clock, and VCO 101 of Walsh's Figure 1 as teaching the claimed LFSR circuit, system clock, and a free-running oscillator, respectively.[6] The Office Action further cites the free-running oscillators 35, exclusive-OR network 20, and flip-flop 16 of Ogrodski's Figure 6 as teaching the claimed plurality of free-running oscillators, single exclusive-OR circuit, and latching circuit, respectively.[7]

The proposed combination does not teach the claimed generator circuit for at least two reasons. First, the proposed combination does not teach the sample clock of Walsh as inputting to the flip-flop 16 of Ogrodski. Thus, the sample clock of Walsh and flip-flop 16 of Ogrodski do not teach the claimed configuration of the LFSR circuit and latching circuit.

Second, the oscillators 35 of Ogrodski are each connected to the same digital noise clock signal source. Similarly, the LFSR circuit 109, VCO 101, and sample circuit 105 of Walsh are also each triggered by the same clock pulse. Thus, in both references, the oscillating devices are triggered by a single clock pulse. As stated above, the claimed oscillators are "free-running" oscillators. Those of ordinary skill in the art know that such "free-running" oscillators operate independently of one another and are not triggered by a clock pulse. It is the lack of any possibility for the "free-running" oscillator to lock on a single clock pulse that helps ensure true random numbers by the LFSR can occur.

[5] Specification, page 2, line 18 – page 3, line 19.
[6] Office Action, 1/29/2004, page 3.
[7] Office Action, 1/29/2004, page 3.

Accordingly, as the proposed combination does not teach the claimed configuration, and as the oscillators of the proposed combination are not "free-running", Applicant respectfully requests that the rejection of Claims 1-3, 5-7, and 10-12, under § 103(a) as unpatentable over Walsh in view of Ogrodski, be withdrawn.

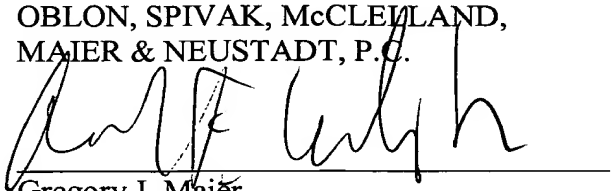
In addition, with respect to the proposed combination of Walsh and Ogrodski, the Office Action states that it would have been obvious to a person of ordinary skill in the art to replace the oscillator of Walsh with a plurality of oscillators, having a lowest common denominator of 1 and feeding an exclusive-OR circuit input to a D-type flip flop, as taught by Ogrodski, because such replacement would improve the randomness of a random number generator. Applicants note that general conclusions concerning what is basic knowledge to one of ordinary skill in the art, without a specific factual finding and concrete evidence in the record to support such a finding, cannot support an obviousness rejection.[8] Therefore, Applicant respectfully requests citation of a reference that teaches the above conclusions. Alternatively, Applicant respectfully requests that the rejection be withdrawn.

[8] MPEP §2144.03B.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599

Raymond F. Cardillo, Jr.
Registration No. 40,440

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/03)
STD/rac

I:\ATTY\STD\20's\206504US\206504US-AM.DOC